intercede

DEVICE AUTHORITY
Edge to Enterprise IoT Security

Whitepaper:

THE ADVANCEMENT OF INTERNET OF MEDICAL THINGS AND THE IMPORTANCE OF SECURE PRIVATE HEALTH INFORMATION

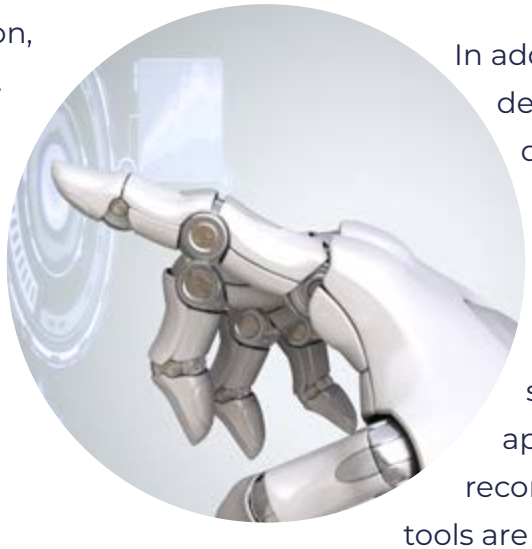
Contents:

The Internet of Medical Things

The Internet of Medical Things (IoMT) has been disrupting the healthcare industry for several years now, not only for patient care/safety, but also for cost savings and operational efficiency. Since COVID appeared, there's been an almost exponential explosion of telemedicine by healthcare systems from pre-COVID levels. This change happened almost overnight as COVID-19 spread. As a result of quarantines and states closing, health systems stopped seeing many patients in person and this trend of remote patient care is not going away.

IoMT devices and their ability to connect with Healthcare IT systems have huge benefits

Utilizing technologies using sensors and Internet of Medical Things (IoMT) make it possible for healthcare personnel to remotely measure patients' vital signs like heart rate, respiratory rate, oxygen saturation, blood pressure, and much more. Another example of connected IoMT in a hospital settings are assistive robot machines. Imagine a doctor conducting surgery on a patient with a surgical robot remotely, without being present other than sending the instructions to the robot securely.



These IoMT devices and their ability to connect to Healthcare IT systems have huge benefits but also have increased the number of cyber risks within the healthcare sector, such as telehealth device flaws, insider threats, and the rise of targeted cyberattacks.

Sensitive data in any application is a gold mine to rogue attackers and adversaries and this is true in medical applications. To properly protect sensitive data, you need to be able to trust both the people and the devices involved. Systems today tend to be either person or device centric, leaving security gaps that can be exploited by attackers.

Anywhere where data must be kept private, such as healthcare, or systems protected, such as critical national infrastructure, needs to be able to trust the devices and the people who access them. IoT devices demand a device centric identity model which is very different from a human / user centric model. Where device trust, data trust and operationalizing trust at scale is a fundamental challenge.

In addition to the wide range of devices involved in healthcare delivery, a similarly diverse set of applications are involved. Along with the standard calendars, communications and messaging software, several healthcare specific applications such as medical records and specialist diagnosis tools are involved in both creating and processing sensitive data. These applications are typically a mix of on premise and SaaS, ranging from modern to legacy and on occasion are customised to a particular healthcare institution or service. Combined

with the fact that the devices themselves are often subject to hardware restrictions to enable them to be used in medical situations (e.g., no USB ports), enabling secure access to systems and devices in the healthcare environment presents one of the most challenging sets of issues in any sector.

Zero Trust

In a world of Zero Trust, where no device or digital identity should be trusted, the healthcare sector has many areas where data breach could be a very real threat.

The US Executive Order on Improving the Nations Cybersecurity (May 2021) ordered the National Institute of Standards and Technology (NIST) to include standards and procedures to enhance the security of the software supply chain including providing the purchaser of software with a Software Bill of Materials (SBOM).

The SBOM lists the components within the software, such as the code used. Understanding the supply chain of software, obtaining an SBOM and analysing it to known vulnerabilities are crucial in managing the risk of data breach.

Managing digital identities and credentials, whether humans or devices is complicated, and you need to be sure that your credential management system and software on your devices are trusted and tested to identify any vulnerabilities and can be updated fast.

So what are the solutions?

By working together, **Intercede** and **Device Authority** can provide an end-to-end solution, securing the devices and protecting access to data.

Device Authorities' KeyScaler IoT IAM platform combines secure device onboarding and provisioning with policy- driven crypto and credential management for IoT PKI automation at scale. Automating identity management for devices and gateways, as well as IoT applications and platforms, such as Microsoft Azure, ThingWorx and AWS IoT. Intercede's MyID solution enables secure digital identities to be issued to people to protect access to networks and systems. Supporting multiple secure access mechanisms, including PKI and FIDO, and a wide range of secure devices, including smart cards, USB tokens, virtual smart cards and mobile devices, MyID enables organisation to mix and match technologies to best fit the system that are being protected and the types of users that need to access them.

Both leaders in their field, Device Authority and Intercede believe a coordinated solution approach combining Device ID and Person ID can significantly improve the level of security and provide the highest level of data protection. All IoT use cases require some form of application, where data is aggregated, whether that's Azure IoT Hub, AWS IoT, ThingWorx or other. Ultimately these applications

need to trust the devices connecting to them and to trust the data being sent from them.

In many scenarios IoT deployments require strict access and protection of data, and only authorize specific users the right to access data. Healthcare is a good example of this, not only do they need these controls in place to protect patient privacy, but Healthcare solutions providers also need to meet compliance and legislation requirements.

HIPPA & PHI

In the US the Health Insurance Portability and Accountability Act (HIPAA) requires companies that deal with protected health information (PHI) to have physical, network and process security measures in place and follow them.

Companies working within the healthcare industry have to adhere to these rules, by ensuring their patients health information is secured and kept private, but is also easily transportable to other providers. The full legislation can be found here.

However, with multiple clinicians having access to patient data across numerous devices that can be somewhat of a challenge.

Assessing the Risks

There are huge benefits for connected devices, but of course there are also concerns and risks associated with connecting any device. Connected medical devices are a good example of this.

Enterprises are concerned with:

- Standards / Compliance
  - Legal
- Security and Privacy
  - Patient health and safety
  - Loss of PHI / data
  - Network attacks Interoperability
- Cost
- Reputation

Connecting devices, people, and systems

It is imperative that people, devices and systems are conneted because it has a particularly strong impact in the healthcare industry.

Up to the second information can mean the difference between life and death for patients, and the potential applications of connected technology to improve care are endless. Pacemakers that doctors can remotely monitor and maintain to identify problems before a heart attack and insulin pumps that can

be adjusted wirelessly, giving a patient more control and better care are already a reality.

As in the digitization of any industry, the same connectivity that drives significant value simultaneously heightens security and privacy risks.

Managing 10 devices is easy, managing 10,000 is hard!

There are a number of common security challenges which IoT vendors see, broadly broken into the following areas:

Provisioning and managing device and user identities at scale

- Creating scalable, distributed trust requires sophisticated PKI implementation
- “Managing 10 devices is easy, managing 10,000 is hard!”

Implementing the correct data protection controls

- Ensuring only authorized entities have access to sensitive data
- “Encryption is easy, managing keys is hard!”

Preventing unauthorized access to devices

- Ensuring all updates and data sent to device are locally verifiable.
- "Controlling access to server resources is easy, doing the same on the device itself is hard!"

The one question that gets asked a lot is:

Who is responsible for security in Healthcare?

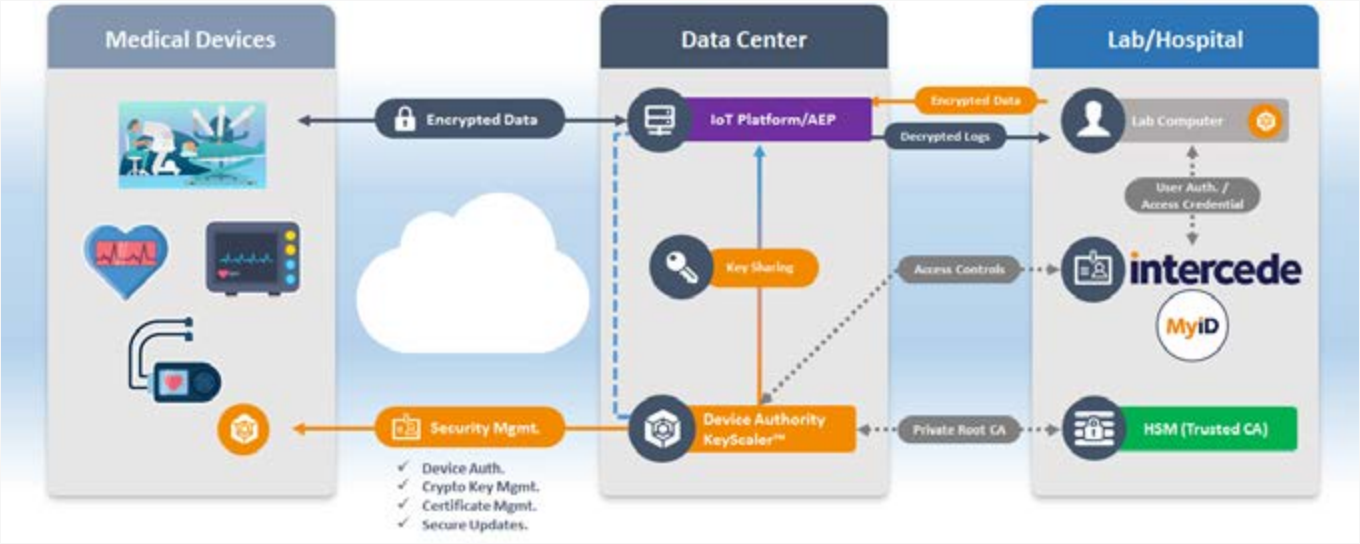
As the worlds of healthcare, wireless connectivity and mobile devices collide, security of the data/ information transmitted needs to be carefully considered. The data being transmitted can vary from very low risk to very high risk, and the means of device design to secure data and authenticate devices must be considered.

To ensure the safety of patient data, the FDA released a new draft guidance that addresses the steps manufacturers must follow in order to protect medical devices against cyberattacks. Device manufacturers and OEM / chip makers and device designers must identify, investigate, and overcome these challenges so that the implementation of smart connected medical technologies can be achieved. Healthcare providers and device manufacturers should share the responsibility.

Cybersecurity throughout device lifecycle

“Manufacturers are encouraged to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment and maintenance of the device.” Source: Postmarket Management of Cybersecurity in Medical Devices, FDA, Dec. 2016

The diagram below shows a typical medical example, where medical devices are being used in either Hospitals, Outpatient care facilities or at home. In this example the requirement is strong identity and integrity of the medical devices, data privacy and integration to an Enterprise HSM for security operations. Authenticating the device to an IoT platform / AEP can be achieved utilizing standardized PKI certificates or cryptographic tokens. Tokens are typically used with platforms that don't rely on certificate-based authentication for identifying devices.



Utilizing Intercede MyID to provide the correct digital identity, credentials, and access controls to a particular user inside the hospital / lab. Any system used for issuing digital identities must be able to do so in a secure manner to ensure that the identities it issues can be trusted.

MyID credential management software is secure by design and proven in the most security sensitive environments Including government, defence, and finance, implementing multiple features to protect information and processes including implementing strong authentication and strict role-based access controls to ensure only authorised individuals can perform credential management activities.

An important feature is the ability to issue multiple types of credentials onto different devices. This enables organisations to use the devices that best fit a particular environment and set of user requirements, examples Include:

- A back-office worker, issued a PKI certificate to a smart card, used with a smart card reader on their desktop PC
- A medical technician, who in their role travels to multiple sites, issued a PKI certificate to a virtual smart card built into their laptop
- A medical career in a clinical environment, issued a USB token with a FIDO credential enabling them to use contactless secure logon to shared devices

- A purchasing officer, using the MyID mobile authentication app, enabling them to sign into Office 365 and authorise purchases straight from their smartphone or tablet.

This ensures that only authorized users have the correct credentials and privileges to access sensitive data and Implement a strong data privacy and security model end to end, from device to authorized user. Protecting the patient's data, meeting compliance and legislation requirements.

A Combined Solution

Device Authority and Intercede enable trust in both devices and people, providing the highest level of data protection and privacy.

Both leaders in their fields, Device Authority bring the device ID expertise and Intercede the Person ID knowledge. By collaborating a combined solution brings device trust, data trust, user trust and end to end security

Managing a flexible range of credentials for IoT Devices and users at scale, proving strong authentication and data protection deployable in complex healthcare environments.

Device and user Identity coupled together to bring end to Edge to cloud trust, data privacy and automation In IoT use cases.

Key Features and Benefits

- Securely register and Identify devices to applications, services and IoT platforms, ensuing only trusted devices are allowed to connect
- Policy driven device credential management, enabling automated lifecycle management at scale
- Cryptographically protected data at rest and in transit providing privacy and protection against data loss
- Protect access to data with digital Identities, ensuring only known and trusted Individuals can access systems

About Us

Intercede is a cybersecurity company with a 25-year track record of delivering credential management solutions to governments, military, healthcare, and major commercial organizations worldwide. The MyID platform manages over 15 million identities, providing a single point for the issuance and management of digital identities using PKI and FIDO across platforms including smart cards, mobile, USB tokens, virtual smart cards, and internet of things (IoT).

Intercede Sales

https://www.intercede.com/contact/

Intercede Support

https://forums.intercede.com

Device Authority is a global leader in identity and access management (IAM) for the Internet of Things (IoT) and focuses on medical/healthcare, industrial, automotive and smart connected devices. Our KeyScaler platform provides trust for IoT devices and the IoT ecosystem to address the challenges of securing the Internet of Things. KeyScaler uses breakthrough technology, including Dynamic Device Key Generation (DDKG) and PKI Signature+ that delivers simplicity and trust to IoT devices. This solution delivers automated device provisioning, authentication, credential management, policy-based end-to-end data security/encryption and secure updates.

Device Authority sales:

https://www.deviceauthority.com/contact

Device Authority Support:

https://support.deviceauthority.com